REMARKS

The Office Action dated August 26, 2005 and the Advisory Action dated October 13, 2005 have been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto. Claim 1 has been amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 10 and 11 have been canceled without prejudice or disclaimer. No new matter has been added and no new issues are raised which require further consideration or search. Claims 1-4, 7-9, 12-17, 19-23 and 27-29 are currently pending in the application and are respectfully submitted for consideration.

In the Office Action, claims 1-4, 7-17, 19-23 and 27-29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tello (U.S. Patent No. 6,463,537) in view of Angelo (U.S. Patent No. 6,370,649). The Office Action took the position that Tello discloses all of the elements of the claims, with the exception of requesting a guess passcode from the manufacturer. The Office Action then relied upon Angelo as allegedly curing this deficiency in Tello. The above rejection is respectfully traversed for the reasons which follow.

Claim 1, upon which claims 2-4 and 7-12 are dependent, recites an apparatus for enabling functionality of a component. The apparatus includes an identification module having an identification number stored therein, a hash function module in communication with the identification module, a host in communication with the identification module, a

guess register in communication with the host, an encryption module in communication with the guess register, and a public key module in communication with the encryption module wherein the public key module has a public key stored therein. The apparatus also includes a comparator in communication with the encryption module and the hash function module, such that the comparator may compare a first bit string to a second bit string to generate a function enable output. The first bit string comprises a ciphertext bit string generated by the encryption module and the second bit string comprises a hash value generated by the hash function module. The apparatus further includes a selecting device for selecting at least one of the function enable output and a bonding option output, the selecting device comprising an OR gate having at least one input for receiving said function enable output and the bonding option output. The host is also configured to communicate with a manufacturer to request a guess passcode corresponding to the identification number stored in the identification module.

Claim 13, upon which claims 14-17 and 19 are dependent, recites a component for selectively enabling functionality of an electronic device. The component includes a means for generating an encrypted bit string, a means for acquiring a guess passcode from a manufacturer, a hash function module in communication with an on board memory that has a predefined identification number stored therein, a means for determining if the encrypted bit string matches the guess passcode, and a means for outputting a functionality enable signal. The means for outputting includes a bonding option circuit, and an OR gate in communication with the bonding option circuit and the

means for determining. The OR gate receives an input from at least one of the bonding option circuit and the means for determining and generates the functionality enable signal therefrom.

Claim 20, upon which claims 21-23 and 27-29 are dependent, recites a method for enabling functionality of an electronic component. The method includes the steps of encrypting a first bit string and a second bit string to generate a third bit string, calculating a fourth bit string, comparing the fourth bit string to the third bit string, and generating a function enable signal in accordance with the comparison. The encrypting step further comprises the step of determining a guess passcode, which includes the step of requesting the guess passcode from a manufacturer. The method further includes the step of selecting at least one of a bonding option output and the function enable signal as a final enable output. The selecting step further comprises the steps of transmitting the bonding option output to an OR gate as a first input, transmitting the function enable signal to the OR gate as a second input, and generating the final enable output from the OR gate in accordance with the first and second inputs.

The prior art has failed to produce enablement methods that are effective against reasonably sophisticated attackers. The claimed invention resolves the limitations of the prior art by providing, in one example, a cryptographic method wherein the secure portions of the method are implemented in electronic or computer products. More specifically, embodiments of the claimed invention implement cryptographic functions for enabling functionality of electronic/computer related components, wherein the

relevant secure key related information is contained within computer hardware in a non-volatile memory device and not within a purely software driven configuration. The claimed invention also provides the ability to conduct secure functionality enablement on electronic/computer related components, wherein a public key for enabling the component is contained onboard and utilized in conjunction with a randomly generated component identifier in order to selectively enable additional functionality of the component.

As will be discussed below, the cited references of Tello and Angelo fail to disclose or suggest the elements of the claims, and therefore fail to provide the advantages and features discussed above.

Tello discloses a modified computer motherboard security and identification system. More specifically, Tello discloses a modified motherboard with a microprocessor based security engine, enabling and disabling circuits, memory buffer circuits, modified BIOS, modified DDL, and a smart card reader and smart cards. Upon startup of the computer, the modified BIOS takes control and allows the security engine microprocessor to look for and read from a smart card in the smart card reader that is connected to the security engine microprocessor. A unique hash number is placed in the smart card during the initial set up of the security system and a complimentary hash number is assigned to the security engine memory. During startup, a software program in the flash memory of the security engine compares the hash numbers in the smart card and

the computer. If these two hash numbers are compliments, the boot up procedure is allowed to continue and access to the computer is allowed.

Angelo discloses a computer system with a self-modifying "fail-safe" password system that allows a manufacturer to securely supply a single-use password to users who lose or misplace a system password. The fail-safe password system utilizes a fail-safe counter, an encryption/decryption algorithm, a manufacturer's public key, and a secure non-volatile memory space. Each time a fail-safe password is entered into the computer system, an application decrypts the fail-safe password and compares the resulting value, which is a hash code, to an internal hash value and increments the fail-safe counter or modifies the seed value when the hashes match. When the fail-safe counter is incremented, the previous fail-safe password is no longer valid.

Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest critical and non-obvious elements of the present claims. For example, Tello and Angelo, whether considered alone or in combination, fail to disclose or suggest a comparator which compares a ciphertext bit string generated by the encryption module with a hash value generated by the hash function module to generate an enable output for the component, as recited in claim 1.

According to certain embodiments of the present invention, as recited in claim 1 and supported by the specification, an identification module 28 is used to store a component identification number. The component identification number is transmitted from identification module 28 to hash function module 29. The hash function module 29

is configured to receive the pre-image input from identification module 28 and output a hash value. The hash value generated by hash function module 29 is transmitted to comparator 20 as a second input 20b. Further, host 18 obtains a guess passcode from the manufacturer and transmits the guess passcode to guess register 19. The guess passcode is then transmitted as clear text to public key encryption module 35 (Specification, page 23, lines 9-23 and Fig. 3).

Additionally, as discussed in the present specification, public key module 34, which contains the public key for the device, transmits the public key to public key encryption module 35. Therefore, public key encryption module 35 receives both the guess passcode and the public key as clear text inputs. These two inputs are processed/encrypted by public key encryption module 35 to generate cipher text at the output thereof. This cipher text is transmitted to the first input 20a of comparator 20. Comparator 20 then compares the cipher text received from the public key encryption module 35 representing the guess passcode with the hash value generated by the hash function module representing the identification number of the component. If the comparator 20 determines that these two values match, then an enable signal is output from comparator 20 indicating that the device 33 has determined that the guess passcode is authentic and that the corresponding functionality of the component should be enabled. The output of comparator 20 is transmitted to an input of OR gate 23, while another input of OR gate 23 is connected to the output of a bonding option circuit 25. Consequently, the manufacturer has the option of enabling the functionality of the component even if the

public key or other information relevant to the enabling process was not programmed into the component at the manufacturing stage of the component (Specification, page 24, lines 1-20 and Fig. 3).

Applicants respectfully submit that Tello and Angelo fails to disclose or suggest the above-discussed configuration, as recited in claim 1. Tello merely discloses that a software program in the flash memory of the security engine compares a hash number in the smart card with a hash number in the computer. If these two hash numbers are compliments, the boot up procedure is allowed to continue and access to the computer is allowed (Tello, Column 5, lines 21-35). Tello does not disclose or suggest comparing a cipher text bit string generated by an encryption module with a hash value generated by a hash function module and generating a function enable output based on the comparison. Specifically, Tello does not teach or suggest "a comparator in communication with said encryption module and said hash function module, wherein said comparator compares a first bit string to a second bit string to generate a function enable output for the component, and wherein said first bit string comprises a ciphertext bit string generated by the encryption module and said second bit string comprises a hash value generated by said hash function module," as recited in claim 1. Although Tello discloses that hash numbers are created from personal information stored in the Identification area (Tello, Column 16, lines 31-34), Tello makes no mention of comparing the hash numbers with a cipher text bit string generated by an encryption module in order to generate a function enable output for the component. Angelo also fails to disclose or suggest this limitation.

Therefore, the combination of Tello and Angelo fails to disclose or suggest a comparator which compares a ciphertext bit string generated by the encryption module with a hash value generated by the hash function module to generate an enable output for the component, as recited in claim 1.

Furthermore, Applicants respectfully submit that Tello and Angelo, whether viewed individually or combined, fail to disclose or suggest "a selecting device for selecting at least one of the function enable output and a bonding option output, said selecting device comprising an OR gate having at least one input for receiving said function enable output and the bonding option output," as recited in claim 1. In the Advisory Action, the Examiner takes the position that Tello teaches a selecting device as the control line (PIDEMIST_CTRL) which is used to disable or enable the primary master IDE slot. Applicants respectfully disagree. The OR gate 305 disclosed in Tello does not receive a function enable output and a bonding option output as its two inputs. Rather, OR gate 305 of Tello receives PIDEMIST_CTRL and FLIP FLOP IC 299 as inputs (see Tello, Fig. 10A). These two inputs do not correspond to the function enable output of the comparator and a bonding option output. According to embodiments of the present invention, as discussed above, if either one of function enabler 32 or bonding option 25 indicates that the functionality is to be enabled, then an enable signal is transmitted from the output of OR gate 23 and is used to initiate the enabling of the desired functionality (Specification, Page 20, lines 10-20). Tello fails to disclose or suggest such a configuration. Angelo also fails to disclose or suggest such an element.

Accordingly, the combination of Tello and Angelo fails to disclose or suggest "a selecting device for selecting at least one of the function enable output and a bonding option output, said selecting device comprising an OR gate having at least one input for receiving said function enable output and the bonding option output," as recited in claim 1.

Therefore, for at least the reasons discussed above, Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest all of the elements of claim 1. As such, Applicants respectfully request that the rejection of claim 1 be withdrawn.

Furthermore, Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest the means for outputting a functionality enable signal, as recited in claim 13. In particular, claim 13 recites that "the means for outputting a functionality enable signal includes a bonding option circuit, and an OR gate in communication with the bonding option circuit and said means for determining." Further, claim 13 recites that "the OR gate receives an input from at least one of said bonding option circuit and said means for determining and generates the functionality enable signal therefrom."

As discussed above, with respect to claim 1, Applicants respectfully assert that both Tello and Angelo fail to disclose or suggest an OR gate which receives an input from at least one of the bonding option circuit and the means for determining and generates the functionality enable signal therefrom. As outlined above, Tello discloses

OR gates receiving inputs from control lines and FLIP FLOP 299. Tello does not disclose or suggest that the OR gates receive inputs from means for determining if the encrypted bit string matches the guess passcode and a bonding option circuit. Furthermore, Tello fails to disclose or suggest that the OR gates generate a functionality enable signal after receiving an input from at least one of the bonding option circuit and the means for determining. Angelo also fails to disclose or suggest such a limitation. Thus, the combination of Tello and Angelo fails to disclose or suggest all of the elements of claim 13.

With respect to claim 20, Applicants respectfully submit that Tello and Angelo, whether taken singly or combined, fail to disclose or suggest the step of selecting at least one of a bonding option output and the function enable signal as a final enable output. Claim 20 further recites that "the selecting step also includes the steps of transmitting the bonding option output to an OR gate as a first input, transmitting the function enable signal to the OR gate as a second input, and generating the final enable output from the OR gate in accordance with the first and second inputs." As discussed above in reference to claims 1 and 13, both Tello and Angelo fail to disclose or suggest an OR gate which receives the bonding option circuit as a first input and the function enable signal as a second input, and in turn generates the final enable output in accordance with the two inputs. Therefore, Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest all of the elements of claim 20.

For at least the reasons discussed above, Applicants respectfully request that the rejection of claims 13 and 20 be withdrawn.

In addition, Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest that the component whose functionality is to be enabled comprises at least one of a network switch and a media access controller, as recited in claims 12, 19 and 29. The Office Action takes the position that Tello discloses this limitation on Column 11, lines 50-52. This section of Tello merely discloses that a control line, ISA_CTRL 271, logically connects the data switch IC 257 to the programmable device 141 which is connected to the security engine microprocessor. Tello fails to disclose or suggest that the functionality of the data switch is to be enabled. Also, it is not clear from the disclosure of Tello that the data switch is a network switch, as recited in the present claims. Furthermore, Tello does not disclose or suggest that the component is a media access controller, as recited in claims 12, 19 and 29. Thus, Applicants respectfully assert that the combination of Tello and Angelo fails to disclose or suggest that the component whose functionality is to be enabled comprises at least one of a network switch and a media access controller. As such, Applicants respectfully request that the rejection of claims 12, 19 and 29 be withdrawn.

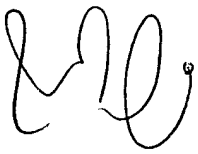
Applicants note that claims 2-4, 7-12, 14-17, 19, 21-23 and 27-29 are dependent upon claims 1, 13, and 20, respectively. Therefore, claims 2-4, 7-12, 14-17, 19, 21-23 and 27-29 should be allowed for at least their dependence upon claims 1, 13, and 20, and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited prior art fails to disclose or suggest critical and important elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-4, 7-17, 19-23, and 27-29 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the Applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802
MSA:jf

Enclosures: Request for Continued Examination